OVERVIEW

Account Hacking or Impersonation

By definition, "business e-mail fraud" occurs when fraudsters gain access to e-mail accounts, especially those of high level executives, and manipulate employees into providing money to accounts controlled by fraudsters. It is also commonly used to refer to scenarios when attackers may not have full control of aforementioned accounts, but impersonate them credibly enough for employees to take action.

While individual cases of internal compromised accounts tend not to make headlines, a recent FBI indictment sheds light on one impersonation scheme which re-routed $120 million from a vendor company to a fraudster. The FBI also detailed an alarming increase in exposed dollar loss over the last 3 years in a recent advisory.

BEST PRACTICE

Cyber Fraud

Resilience's Cyber Meteorology Framework models cyber risk trends and helps companies stay up-to-date with current best practices and mitigation guidance. Resilience's business email fraud model recommend that organizations do the following to prevent and mitigate these attacks:

1. Employ an Email Gateway and conduct periodic phishing awareness training and tests
2. Implement best practices for e-mail settings such as DMARC, DKIM, and SPF
3. Employ Multi Factor Authentication, most critically for the organization's primary e-mail provider.

INSURANCE

Privacy and Fraud

Business email fraud is one of the most common causes of cyber loss. Insurance should not just cover costs to investigate and resolve the security incidents, but also evaluate any privacy exposure, and cover financial losses caused by fraudulent wire transfers and invoice manipulation. Ask your broker for more detail.

Example Claim

A financial services company was the victim of a business email fraud event, which resulted in two fraudulent wire transfers, each for $250,000. The fund transfers were requested from their "alleged" vendor. It was ultimately discovered that the two wire transfers were fraudulent when the company was notified by the real vendor that they had not received the funds. The email accounts compromised also

contained personally identifiable information, as a result implicating privacy law concerns.